Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт кибернетики
Направление подготовки 09.04.01 Информатика и вычислительная техника
Кафедра вычислительной техники

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Разработка и модернизация программно-аппаратного комплекса обеспечения информационной безопасности

УДК _____

Студент

Группа	ФИО	Подпись	Дата
8ВМ4А	Бахтин Артём Олегович		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент	Шерстнев Владислав Станиславович	к.т.н.		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент	Конотопский Владимир Юрьевич	к.э.н.		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
ассистент	Акулов Петр Анатольевич			

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
ВТ	Марков Н.Г.	д.т.н., профессор		

Томск – 2016г.

Таблица 1 – Планируемые результаты обучения по ООП

Код результата	Результат обучения (выпускник должен обладать следующими компетенциями)
Общекультурные компетенции	
ОК-1	владеет культурой мышления, способен к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения
ОК-2	умеет логически верно, аргументировано и ясно строить устную и письменную речь
ОК-3	готов к кооперации с коллегами, работе в коллективе
ОК-4	способен находить организационно-управленческие решения в нестандартных ситуациях и готов нести за них ответственность
ОК-5	умеет использовать нормативные правовые документы в своей деятельности
ОК-6	стремится к саморазвитию, повышению своей квалификации и мастерства
ОК-7	умеет критически оценивать свои достоинства и недостатки, наметить пути и выбрать средства развития достоинств и устранения недостатков
ОК-8	осознает социальную значимость своей будущей профессии, обладает высокой мотивацией к выполнению профессиональной деятельности
ОК-9	способен анализировать социально-значимые проблемы и процессы
ОК-10	использует основные законы естественнонаучных дисциплин в профессиональной деятельности, применяет методы математического анализа и моделирования, теоретического и экспериментального исследования
ОК-11	осознает сущность и значение информации в развитии современного общества; владеет основными методами, способами и средствами получения, хранения, переработки информации
ОК-12	имеет навыки работы с компьютером как средством управления информацией
ОК-13	способен работать с информацией в глобальных компьютерных сетях
ОК-14	владеет одним из иностранных языков на уровне не ниже разговорного
ОК-15	владеет основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий

Продолжение таблицы 1

Профессиональные компетенции	
ПК-1	разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием
ПК-2	осваивать методики использования программных средств для решения практических задач
ПК-3	разрабатывать интерфейсы "человек – электронно-вычислительная машина"
ПК-4	разрабатывать модели компонентов информационных систем, включая модели баз данных
ПК-5	разрабатывать компоненты программных комплексов и баз данных, использовать современные инструментальные средства и технологии программирования
ПК-6	обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности
ПК-7	готовить презентации, научно-технические отчеты по результатам выполненной работы, оформлять результаты исследований в виде статей и докладов на научно-технических конференциях
ПК-8	готовить конспекты и проводить занятия по обучению сотрудников применению программно-методических комплексов, используемых на предприятии
ПК-9	участвовать в настройке и наладке программно-аппаратных комплексов
ПК-10	сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем
ПК-11	инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт Кибернетики
Направление подготовки 09.04.01 Информатика и вычислительная техника
Кафедра Вычислительной техники

УТВЕРЖДАЮ
Зав. кафедрой

_____ _____ Марков Н.Г.
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение квалификационной работы

В форме:

магистерской диссертации

(бакалаврской работы, дипломного проекта/работы, магистерской диссертации)

Студенту:

Группа	**ФИО**
8ВМ4А	Бахтин Артём Олегович

Тема работы:

Разработка и модернизация программно-аппаратного комплекса обеспечения информационной безопасности	
Утверждена приказом директора (дата, номер)	

Срок сдачи студентом выполненной работы:	

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе	Объект исследования: оборудование ЛВС (активное и пассивное), терминальные устройства, устройства обеспечения безопасности (системы обнаружения и предотвращения вторжений), расположенное в учебных корпусах ТПУ

Перечень подлежащих исследованию вопросов	Анализ и модернизация сетевой инфраструктуры ТПУ. Разработка модели и макета устройства обнаружения несанкционированного подключения в проводную линию связи
Перечень графического материала	–

Консультанты по разделам выпускной квалификационной работы

Раздел	**Консультант**
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	Конотопский Владимир Юрьевич
Социальная ответственность	Акулов Петр Анатольевич

Названия разделов, которые должны быть написаны на русском и иностранном языках:

Разработка модели вычислительной сети

Дата выдачи задания на выполнения выпускной квалификационной работы по линейному графику	

Задание выдал руководитель:

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Доцент	Шерстнев Владислав Станиславович	кандидат технических наук		

Задание принял к исполнению студент:

Группа	**ФИО**	**Подпись**	**Дата**
8ВМ4А	Бахтин Артём Олегович		

Министерство образования и науки Российской Федерации

федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт _____
Направление подготовки (специальность)_____
Уровень образования _____
Кафедра _____
Период выполнения _____(осенний / весенний семестр 2015/2016 учебного года)

Форма представления работы:

магистерская диссертация

(бакалаврская работа, дипломный проект/работа, магистерская диссертация)

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН
выполнения выпускной квалификационной работы

Срок сдачи студентом выполненной работы:	

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
11.02.2016	Аналитический обзор методов и средств обеспечения информационной безопасности	*15*
17.03.2016	Разработка модели вычислительной сети	*25*
25.04.2016	Разработка устройства детектирования несанкционированного доступа в ЛВС	*25*
18.05.2016	Результаты проведенного исследования	*15*
01.06.2016	Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	*10*
03.06.2016	Социальная ответственность	*10*

Составил преподаватель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент	Шерстнев В.С.	к.т.н		

СОГЛАСОВАНО:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
ВТ	Марков Н.Г.	д.т.н., профессор		

Реферат

В данной работе производится анализ архитектуры, конфигурационных файлов сетевого оборудования ТПУ. На его основе приводятся доводы в пользы модернизации сетевой инфраструктуры с целью улучшения качественных характеристик. Среди них: повышение удобства администрирования, улучшение масштабируемости и производительности, повышение уровня защищенности сети в целом.

В ходе работе также осуществлена разработка модели и макета устройства, позволяющего обнаруживать несанкционированное подключение в проводную линию связи, работающую по протоколу Ethernet. Описаны возможные пути практического применения данного макета и интеграция его с существующим оборудованием.

Ключевые слова: ЛВС, информационная безопасность, коммутатор, маршрутизатор, OSPF, VLAN, VPN, MPLS, Arduino, телеграфные уравнения длинных линий

Определения, обозначения, сокращения

Определения

DHCP – сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

DHCP Snooping – функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP.

MPLS – механизм в высокопроизводительной телекоммуникационной сети, осуществляющий передачу данных от одного узла сети к другому с помощью меток.

VLAN – группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам.

Виртуальная машина – программная и/или аппаратная система, эмулирующая аппаратное обеспечение некоторой платформы.

Гипервизор – программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких операционных систем на одном и том же хост-компьютере.

Протокол маршрутизации – сетевой протокол, используемый маршрутизаторами для определения возможных маршрутов следования данных в составной компьютерной сети.

Хоп – участок сети между двумя узлами сети, по которому передаются сетевые пакеты (или датаграммы).

Широковещательный домен – группа доменов коллизий, соединенных с помощью устройств второго уровня.

Обозначения и сокращения

Устройство – устройство детектирования несанкционированного доступа к локальной вычислительной сети

УК-10 – учебный корпус №10

УК-Юрга – учебный корпус в г. Юрга

Оглавление

Введение

В феврале 2016 года неизвестные совершили попытку хищения денежных средств у центрального банка Республики Бангладеш в размере 951 миллион долларов. Злоумышленники проникли в сеть банка и проэксплуатировали уязвимость в ПО клиента международной системы денежных переводов SWIFT. Но из-за досадной орфографической ошибки злоумышленники смогли похитить «всего» 81 миллион. Как показало расследование, атака стала возможной благодаря тому, что банк использовал в качестве маршрутизирующего и коммутационного оборудования дешевые устройства стоимостью менее десяти долларов. Также отсутствовал межсетевой экран.

Примеры описания таких и подобных случаев можно во множестве найти в заголовках СМИ. Борьба с атаками на информационные системы и вычислительные сети (далее – сети), и учет рисков, связанных с такими атаками стала неотъемлемой частью стратегии любой более или менее крупной компании, оперирующей персональными данными или имеющей дело с деньгами. Большую часть планов злоумышленников можно сорвать уже на подступах к информационной системе. Для этого должен быть выстроен и регулярно поддерживаться надежный периметр из грамотно сконфигурированных устройств защиты сети.

Целью данной работы является сбор информации о текущей конфигурации сетевых устройств ТПУ, их анализ и предложение внесения изменений в инфраструктуру для повышения удобства администрирования, защищенности, производительности и масштабируемости.

Задача исследования состоит из нескольких этапов:

– подготовительный – обзор литературы с целью изучения лучших практик, применяемых при проектировании и эксплуатации вычислительной сети;

– сбор информации об оборудовании;

– анализ полученной информации с целью выявления недостатков конфигурации, которые влияют на производительность, удобство обслуживания и безопасность сети в целом;

– выдвижение предложений для устранения найденных недостатков, их тестирование на модели;

Для решения поставленных задач предполагается привлечение сотрудников и студентов кафедры ВТ института кибернетики ТПУ.

Объектом исследования данной работы является оборудование ЛВС (активное и пассивное), терминальные устройства, устройства обеспечения безопасности (системы обнаружения и предотвращения вторжений), расположенное в учебных корпусах ТПУ.

В качестве предмета исследования было выбрано совокупность влияния внешних и внутренних факторов на производительность, безопасность, удобство обслуживания сети. Предполагается также разработка прототипа устройства для обнаружения несанкционированного подключения в проводную линию ЛВС и постройка на его основе коммутационного шкафа для централизованного сбора подобной статистики и отправки ее на сервер логирования.

В ходе работы необходимо обобщить существующие знания и применить лучшие практики по проектированию, конфигурированию и эксплуатации сетевых и терминальных устройств. Для разработки устройства детектирования предполагается провести поиск аналогов в смежных технических областях. Например, такой, как детектирование места обрыва на магистральных высоковольтных ЛЭП. После поиска подобных конкурирующих решений можно будет сделать вывод о том применении ранее такого подхода в смежных областях.

Результаты ВКР являются практически значимыми для областей, где требуется вести мониторинг проводных линий связи на предмет обрыва/несанкционированного вторжения. Разработанная архитектура сети может быть в дальнейшем усовершенствована и применена для решения задач построения сложных, разветвленных систем.

По теме исследования были написаны 2 статьи. Одна из них по теме «Shellshock bash interpreter vulnerability analysis» опубликована в журнале «Современные наукоемкие технологии» (входящим в список изданий, рекомендуемых ВАК для защиты кандидатских и докторских диссертаций). Вторая – с темой «Detection of an Unauthorized Wired Connection to a Local Area Network by Solving Telegraph Equations System» представлена на XII Международной Сибирской конференции по управлению и связи (SIBCON-2016) при поддержке IEEE и опубликована в сборнике докладов конференции.

Прототип устройства детектирования несанкционированного доступа в ЛВС был представлен членам жюри на Первом всероссийском Хакатоне по тематике «Промышленные сети», проводимом компанией CISCO в г. Екатеринбург 20-22 апреля 2016г.

1 Аналитический обзор методов и средств обеспечения информационной безопасности

В данном разделе приводятся сведения о текущем состоянии решаемой проблемы, достижениях современной науки и техники в рассматриваемой области технологий. Приведены также ссылки на источники информации, в т. ч. из сети Интернет. В главе 1.1 описаны современные способы решения проблемы разделения крупной сети на подсети. В главе 1.2 приведен сравнительный анализ динамических протоколов маршрутизации. В главе 1.3 рассматриваются средства организации сетевого периметра. В главе 1.4 описаны способы атак на проводную линию связи.

Исследуемая область достаточно хорошо освещена во множестве литературных источниках. Большое количество ресурсов в сети Интернет посвящены настройке сетевого оборудования. Есть также авторитетные источники, описывающие процедуру проектирования крупных ЛВС. Такое обилие информации зачастую сложно поддается обработке и компиляции из нее нужных знаний. Источники могут противоречить друг другу. Разные производители оборудования предлагают использовать свои, зачастую проприетарные технологии, которые плохо стыкуются с другими вендорами. [1] Такое многообразие и плохая совместимость технологий часто становится решающим в принятии решения о выборе единого производителя для построения сети. Различия в технологиях снижают удобство централизованного обслуживания, а иногда и становятся источниками проблем с безопасностью. Существуют даже компании, которые строят свой бизнес на таком различии технологий, предлагая решения для управления оборудованием разных производителей. [2] Таким образом, задача проектирования сети и поиск недостатков в прошлых конфигурациях сводилась к компиляции лучших практик, описанных в многочисленных руководствах по настройки оборудования вендоров. Требовалось также проанализировать источники на предмет возможности эксплуатации недостатков конфигура-

ции с целью получения неавторизованного доступа к ресурсам сети и привилегиям администратора.

1.1 Применяемые методы при решении задачи организации подсетей

Рассмотрим подходы, которые применяются при решении задачи деления крупной сети на подсети. Проведем краткий обзор технологий.

Во времена использования классовой адресации и отсутствии коммутаторов проблема организации подсетей решалась весьма просто. Организация получала у провайдера блок публичных адресов определенной длины и использовала его по своему усмотрению. Чаще всего – делила на блоки меньшей длины для создания подсетей. От такой практики пришлось отойти с началом нехватки публичных адресов пространства IPv4, приходом бесклассовой адресации и появлении коммутаторов. Организации стали использовать приватные адреса для сокращения количества используемых публичных адресов, переносить подсети за устройства динамической трансляции адресов (NAT) и разделять их с помощью коммутаторов. Такая конфигурация удобна до тех пор, пока количество подсетей не начинает расти. Для этого приходится применять все большее количество устройств коммутации, администрирование становится все сложней. Ситуация изменилась с приходом технологии VLAN – разделения сети на виртуальные подсети, которые не требуют физического разграничения устройствами маршрутизации. Такой подход также сокращает издержки на администрирование сети, т.к. в большинстве случаев сети терминируются на одном маршрутизаторе. Также дает возможность более гибкой конфигурации клиентов подсети. Так, например, перенос одного клиента в другую подсеть более не требует физического переключения его на другой порт, а всего лишь изменения пары строчек в файле конфигурации. [3] На данном этапе развития сетей такой метод деления на подсети является самым широко используемым. Более того, подход логического разделения клиентов на устройстве является одной из составных частей эволюционного развития технологии проектирова-

ния – программно-определяемых сетей, в которых потоки трафика определяются с помощью абстрактного программного обеспечения. [4]

Таким образом, можно говорить о том, что основным средством деления на подсети в настоящее время является технология VLAN. Для сокращения количества используемых публичных адресов применяется технология NAT.

1.2 Протоколы, используемые при решении задачи организации динамической маршрутизации сети

Рассмотрим динамические протоколы маршрутизации, проведем анализ их функциональных возможностей, алгоритмов работы и областей применения.

Динамическая маршрутизация пришла на замену статическим методам по ряду причин. Основными из них являются удобство и скорость администрирования и конфигурирования. Что в свою очередь снижает возможность возникновения ошибок, вызванных человеческим фактором. Для проведения сравнительного анализа используемых протоколов и их функциональных возможностей приведем таблицу (Таблица 2). [5]

Таблица 2 – Сравнительная таблица функциональных возможностей динамических протоколов маршрутизации

Наименование	Тип	Проприетарность	Функция	Период обновлений	Метрика	VLSM	суммирование маршрута
RIP	дистанционно-векторный	нет	внутренний шлюз	30с	хоп	нет	автоматически
RIPv2	дистанционно-векторный	нет	внутренний шлюз	30с	хоп	да	автоматически
IGRP	дистанционно-векторный	да	внутренний шлюз	90с	композитная	нет	автоматически
EIGRP	расширенный дистанционно-векторный	да	внутренний шлюз	по событию	композитная	да	автоматически/вручную
OSPF	состояние канала	нет	внутренний шлюз	по событию	стоимость	да	вручную

Продолжение таблицы 2

IS-IS	состояние канала	нет	внутренний шлюз	по событию	стоимость	да	автоматически
BGP	дистанционно-векторный	нет	внешний шлюз	инкрементальное	н/п	да	автоматически

Протокол RIP не поддерживает масок переменной длины. В современных условиях этот протокол можно считать неприменимым и морально-устаревшим. Протокол RIPv2 до сих пор используется в некоторых организациях с небольшим потоком трафика и небольшим количеством устройств. Но тоже уже встречается довольно редко в силу своей низкой скорости сходимости – 30с. Протокол IGRP – это проприетарный протокол, который был разработан компанией Cisco для того, чтобы преодолеть ограничения протокола RIP на максимальное количество хостов. В настоящее время не используется, т.к. не поддерживает сетевых масок переменной длины. Пришедший ему на замену, также проприетарный, протокол EIGRP используется в гомогенных сетях одного вендора. Т.к. реализация этого протокола присутствует не на всем оборудовании в силу своей закрытости. Отличительной особенностью протокола является продвинутый алгоритм вычисления метрики маршрута, в основу которого положены два критерия: минимальная пропускная способность данного маршрута и загрузка и надежность маршрутов на пути следования пакета. В общем случае производительность протокола схожа с OSPF.

Протокол OSPF в настоящее время является одним из самых распространенных протоколов маршрутизации внутри одной автономной системы. Для нахождения кратчайшего маршрута он использует алгоритм Дейкстры. В отличие от дистанционно-векторных протоколов обладает более высокой скоростью сходимости, использует информацию о пропускной способности каждого соединения. OSPF используется в сетях малого и среднего размера.

С использованием протокола IS-IS строятся сети крупных провайдеров услуг и особо крупных корпоративных сетях. Как и протокол OSPF, IS-IS использует информацию о состоянии соединений, что повышает эффективность

утилизации вычислительных ресурсов оборудования. Так же использует алгоритм Дейкстры для расчета оптимального маршрута.

Протокол BGP относится к классу протоколов маршрутизации на основе внешнего шлюза. Это предполагает использование его для обмена информацией о достижимости между автономными системами. Выбор наилучшего маршрута определяется по правилам, принятым в конкретной сети.

Таким образом, протоколы динамической маршрутизации можно глобально разделить на две части: протокол маршрутизации внутреннего (IGP) и внешнего (EGP) шлюза. Каждый из них имеет свою специфику применения и случаи, в которых стоит использовать тот или иной протокол. Современными вариантами IGP являются протоколы OSPF, EIGRP, IS-IS. Самым распространённым протоколом EGP в настоящее время является протокол BGP.

1.3 Средства организации защиты сетевого периметра

Рассмотрим современные средства организации защиты сетевого периметра организации и специфику их применения.

Организация защиты периметра считается обязательным этапом при проектировании корпоративной сети. Зачастую он включает в себя средства межсетевого экранирования, организацию защищенных туннелей (VPN), а также средства глубокого анализа трафика – системы обнаружения и предотвращения вторжений (IDS/IPS). Межсетевой экран с правильно настроенной конфигурацией является первой линией защиты от атак на сеть. На смену межсетевым экранам с фильтрацией пакетов, осуществляющих блокировку только по портам и адресам, пришли новые устройства, действующие на уровне приложения. Помимо функции непосредственной фильтрации межсетевые экраны зачастую выполняют функцию защищенного соединения между территориально удаленными площадками.

Считается, что понятие «сетевой периметр» в чистом виде устарело. Это связано с увеличением числа мобильных устройств у сотрудников организации

и приходом облачных технологий. Многие компании сегодня переносят свою ИТ и ИБ инфраструктуру в такие «облака», размывая при этом границы периметра. Возрастающее количество мобильных устройств и тенденция к хранению на них корпоративных данных вынуждает ИТ департаменты компаний вводить специальные на этот счет политики. Появились специальные программные продукты, которые позволяют организовывать на устройствах защищенные контролируемые контейнеры, в которых можно безопасно хранить корпоративные данные без угрозы их утечки, в случае утери мобильного устройства. Методы организации таких контейнеров постоянно эволюционируют вместе с вредоносным ПО, которое направлено на извлечение из них данных.

Для защищенного удаленного подключения чаще всего организовывается VPN-туннель. Он также часто применяется и на мобильных устройствах для безопасного подключения к сети организации для работы с корпоративными данными. [6]

Таким образом, можно говорить о том, что основными средствами организации сетевого периметра и по сей день остаются устройства межсетевого экранирования. Хотя провести четкий периметр становится все сложнее из-за все увеличивающегося количество персональных мобильных устройств, на которых сотрудники склонны хранить персональную информацию.

1.4 Методы атак на проводные линии связи

В данной главе рассмотрим и приведем категории атак на проводные линии связи. Покажем актуальность проблемы и методы ее решения.

По способу взаимодействия на канал связи атаки можно условно разделить на:

– пассивные. Злоумышленник не имеет возможности модифицировать проходящий через него трафик;

– отказ в обслуживании. Целью данной атаки является нарушение работоспособности предоставляемых в сети сервисов;

– «человек посередине». При такой атаке возможна модификация данных, изменение порядка сообщений;

– фальсификация. Метод, при котором злоумышленник пытается выдать себя за другого субъекта;

– повторное использование. Атака с пассивным захватом сообщений и повторным их использованием с целью фальсификации.

Все вышеперечисленные методы активно используются и комбинируются при атаках на линии связи. Самым очевидным и простым решением для защиты от снятия информации с каналов связи является шифрование передаваемых по ним данным. Но статистика по количеству шифруемого трафика говорит о том, что не все организации прибегают к таким мерам. Так по статистике компании Sandvine доля зашифрованного трафика в Северной Америке за апрель 2015г. составляла всего 29.1% от общего потока. (Рисунок 1) Большая часть из этих данных плохо защищена не только во время передачи, но также и во время хранения [7]

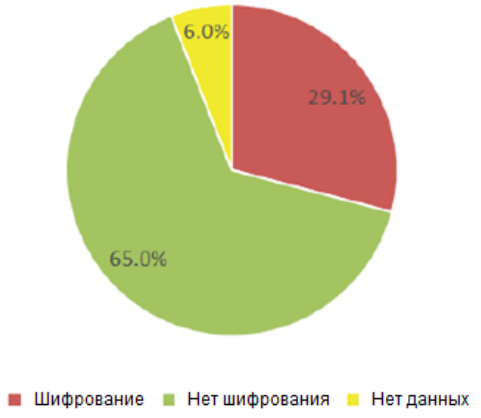

Рисунок 1 – Доля зашифрованного трафика

Многочисленные информационные поводы в СМИ, которые освещают события, связанные с прослушиванием линий связи, в т. ч. и высокопоставленных чиновников, а также вышеприведенная статистика натолкнули на мысль о попытке создания Устройства.

Рассмотрим способы, которыми пользуются специалисты в области защиты информации, а также, перенимающие и адаптирующие их наработки, злоумышленники. Наиболее распространенным, самым легким и дешевым в эксплуатации способом является подключение в разрыв линии связи. Существует даже коммерческие устройства для осуществления такого подключения. [8] Внешний вид такого устройства приведен на рисунке (Рисунок 2).

Рисунок 2 – Внешний вид устройства для подключения в разрыв линии связи

Работает данное и все похожие устройства следующим образом. В противоположные разъемы подключается место разрыва кабеля. Конечно, для начала злоумышленнику необходимо разорвать (разрезать) канал связи и оконечить его в соответствии со стандартами обжима кабеля. Именно в этот момент чаще всего и обнаруживается такая атака. В два других разъема подключается прослушивающее устройство. Чаще всего таким устройством является сетевая карта(либо встроенная в ПК, либо выполненная отдельным устройством). Причем, один разъем может прослушивать одновременно только одно направление передачи: либо из точки А в В, либо наоборот. Для того, чтобы прослушивать одновременно два направления необходимо две сетевые карты. Для того чтобы запустить режим прослушивания на сетевой карте, необходимо перевести её в неразборчивый режим (promiscious mode). В таком режиме сетевое устройство принимает все Ethernet-кадры, которые попадают на её интерфейс. В отличие от нормального режима работы, когда карта принимает только те кадры, которые предназначены данному физическому устройству с данным физическим(MAC) адресом. Стоит также отметить тот факт, что злоумышлен-

ник никак не выдает себя, так как не может посылать кадры в сеть ввиду отсутствия таковой физической возможности – отсутствует необходимая для передачи пара проводников.

Весь незащищенный трафик злоумышленник может разбирать с помощью сетевых анализаторов. Самые известные из них: Wireshark, tcpdump. Процесс разбора сетевых кадров с помощью утилиты Wireshark представлен на рисунке. (Рисунок 3)

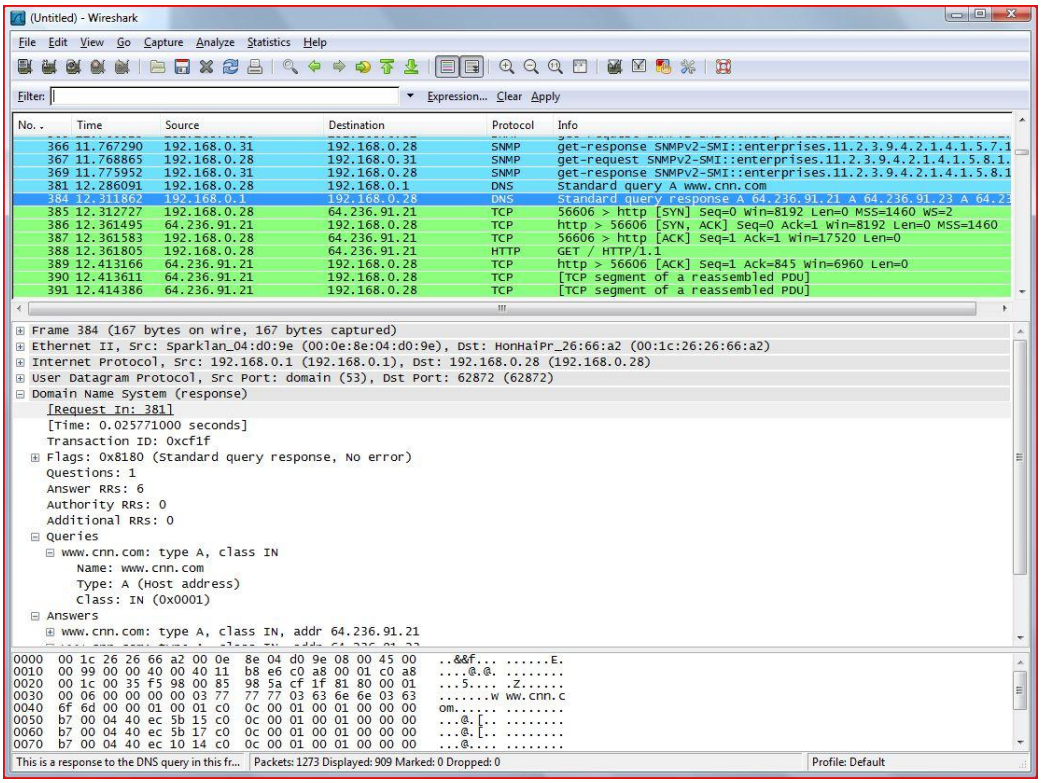

Рисунок 3 – Процесс анализа сетевого трафика с помощью утилиты Wireshark

При проектировании Устройства требовалось провести анализ рынка уже существующих подобных устройств. Так, в ходе этого анализа, был обнаружен патент на устройство детектирования обрыва в проводной линии связи, использующей пакетную технологию Ethernet. Патент, в частности, подан от имени ЗАО НПЦ «Компьютерные технологии». На сайте компании можно найти предложения по мониторингу линий связи для провайдеров. [9] Оборудование, производимое данной компанией, позволяет обнаруживать обрыв и отправлять диагностическое сообщение в систему мониторинга. Похожие

устройства также эксплуатируются в смежных областях исследования – на магистральных высоковольтных ЛЭП. [10]

Таким образом, можно сделать вывод о том, что хотя и существуют надежные программно-аппаратные средства, которые решают проблему прослушивания канала связи, большая часть данных передается в незашифрованном виде. Этим пользуются злоумышленники. Для организации атаки не требуется глубоких знаний по данной тематике. Это усугубляется еще и тем фактом, что компании, чей трафик содержит много конфиденциальной информации, крайне мало уделяют внимания защите от подобных видов атак.

1.5 Выводы по главе

В данном разделе было проведено аналитическое исследование методов и средств обеспечения информационной безопасности. Сделан обзор различных технологий, которые применяются при решении задач организации подсетей, динамической маршрутизации в сети, организации защиты сетевого периметра. Рассмотрены методы атак на проводные линии связи. Используя полученные знания можно переходить к сбору информации о текущей конфигурации сети, ее анализу и выявления недостатков с целью их исправления.

ЗАДАНИЕ ДЛЯ РАЗДЕЛА «ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
8ВМ4А	Бахтин Артём Олегович

Институт	Кибернетики	Кафедра	ВТ
Уровень образования	Магистратура	Направление/специальность	Информатика и вычислительная техника

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. *Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих* 2. *Нормы и нормативы расходования ресурсов* 3. *Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования*	*Работа с информацией, представленной в российских и иностранных научных публикациях, интернет ресурсах, аналитических материалах, нормативно-правовых документах.*
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Организация и планирование работ выполнения проекта*	1. *Расчет продолжительности работ* 2. *Расчет накопления готовности проекта*
2. *Расчет сметы затрат на выполнение проекта*	1. *Расчет затрат на материалы, заработной платы, социальный налог, затрат на электроэнергию* 2. *Расчет амортизационных расходов, расходов на основе платежных документов и прочих расходов* 3. *Расчет общей себестоимости разработки, прибыли, НДС*
3. *Оценка экономической эффективности проекта*	1. *Оценка экономической эффективности и научно – технического уровня НИР*
Перечень графического материала *(с точным указанием обязательных чертежей):*	
1. *Линейный график работ*	

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент	Конотопский В.Ю.	к.э.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ4А	Бахтин Артём Олегович		

2 Финансовый менеджмент, ресурсоэффективность и ресурсосбережение

Целью данного раздела является комплексное описание и анализ финансово-экономических аспектов выполненной работы. Оценка полных денежных затрат на проект, а также приближенная экономическая оценка результатов его внедрения. Приведена также оценка экономической целесообразности осуществления работы. Раздел завершен комплексной оценкой научно-технического уровня ВКР на основе экспертных данных.

2.1 Организация и планирование работ

2.1.1 Продолжительность этапов работ

В данном пункте составляется полный перечень проводимых работ, определяются их исполнители и рациональная продолжительность. Наглядным результатом планирования работ является линейный график реализации проекта.

Расчет продолжительности этапов работ осуществляется опытно-статистическим методом, экспертным способом. Оценка таким способом опирается на профессиональный опыт и эрудицию эксперта. Для определения вероятных (ожидаемых) значений продолжительности работ $t_{ож}$ применяется следующая формула:

$$t_{ожс} = \frac{3 \cdot t_{\min} + 2 \cdot t_{\max}}{5} \quad (2.1)$$

Исполнители: ИР – инженер-разработчик, ИВ – инженер по внедрению

В таблице 3 приведен перечень работ и продолжительность их выполнения.

Таблица 3 – Перечень работ и продолжительность их выполнения

Этапы работы	**Исполнители**	**Загрузка исполнителей**
Получение исходных данных (логическая, физическая, информационная топология сети, файлы конфигураций)	ИР	ИР – 100%
Составление и утверждение ТЗ	ИР	ИР – 100%
Изучение функциональных характеристик существующего оборудования, линий связи, используемых протоколов	ИР	ИР – 100%
Изучение конфигурационных файлов устройств. Поиск ошибок конфигурации топологии, оборудования	ИР	ИР – 100%
Изучение текущего состояния рынка сетевого оборудования, протоколов. Изучение возможности замены устаревшего оборудования на новое.	ИР	ИР – 100%
Составление модели сети с учетом внесенных исправлений в её архитектуру.	ИР	ИР – 100%
Тестирование модели сети. Устранение ошибок.	ИР, ИВ	НР – 50% ИВ – 50%
Разработка плана внедрения проекта у заказчика. Составление сопроводительной документации.	ИР, ИВ	ИР – 30% ИВ – 70%
Монтажные работы (установка оборудования, прокладка линий связи)	ИР, ИВ	ИР – 40% ИВ – 60%
Тестирование новой конфигурации	ИВ	ИВ – 100%
Сдача проекта заказчику	ИВ	ИВ – 100%

Расчет продолжительности выполнения каждого этапа в рабочих днях (***$T_{РД}$***) ведется по формуле:

$$\mathrm{T_{РД}} = \frac{\mathrm{t_{ож}}}{\mathrm{K_{ВН}}} \cdot \mathrm{K_Д} \qquad (2.2)$$

где $t_{ож}$ – продолжительность работы, дн.;

$K_{вн}$ – коэффициент выполнения работ, учитывающий влияние внешних факторов на соблюдение предварительно определенных длительностей, $K_{вн} = 1$;

$K_Д$ – коэффициент, учитывающий дополнительное время на компенсацию непредвиденных задержек и согласование работ, $K_Д = 1$.

Расчет продолжительности этапа в календарных днях ведется по формуле:

$$T_{КД} = T_{РД} \cdot T_{К}, \quad (2.3)$$

где $T_{КД}$ – продолжительность выполнения этапа в календарных днях;

$T_{К}$ – коэффициент календарности, позволяющий перейти от длительности работ в рабочих днях к их аналогам в календарных днях, $T_{К}$ = 1.4. В таблице 4 приведены продолжительности этапов работ и их трудоемкости по исполнителям, занятым на каждом этапе.

Таблица 4 – Трудозатраты на выполнение проекта

Этап	Исполнители	Продолжительность работ, дни			Трудоемкость работ по исполнителям чел.-дн.			
					$T_{РД}$		$T_{КД}$	
		t_{min}	t_{max}	$t_{ож}$	ИР	ИВ	ИР	ИВ
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Получение исходных данных (логическая, физическая, информационная топология сети, файлы конфигураций)	ИР	1	4	2.2	2.64	–	3.70	–
Составление и утверждение ТЗ	ИР	4	6	4.8	5.76	–	8.06	–
Изучение функциональных характеристик существующего оборудования, линий связи, используемых протоколов	ИР	4	6	4.8	5.76	–	8.06	–
Изучение конфигурационных файлов устройств. Поиск ошибок конфигурации топологии, оборудования	ИР	11	16	13	15.60	–	21.84	–
Изучение текущего состояния рынка сетевого оборудования, протоколов. Изучение возможности замены устаревшего оборудования на новое.	ИР	7	11	8.6	10.32	–	14.45	–
Составление модели сети с учетом внесенных исправлений в её архитектуру.	ИР	22	27	24	28.80	–	40.32	–
Тестирование модели сети. Устранение ошибок.	ИР, ИВ	6	9	7.2	4.32	4.32	6.05	6.05
Разработка плана внедрения проекта у заказчика. Составление сопроводительной документации.	ИР, ИВ	15	18	16.2	5.83	13.61	8.16	19.05
Монтажные работы (установка оборудования, прокладка линий связи)	ИР, ИВ	21	30	24.6	11.81	17.71	16.53	24.80
Тестирование новой конфигурации	ИВ	5	6	5.4	–	6.48	–	9.07
Сдача проекта заказчику	ИВ	2	4	2.8	–	3.36	–	4.70
Итого:				**118.6**	**96.84**	**45.48**	**127.18**	**63.67**

Таблица 5 – Линейный график работ

Этап	**ИР**	**ИВ**	Февраль			Март			Апрель			Май			Июнь			Июль
			10	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**	**110**	**120**	**130**	**140**	**150**	**160**
1	3.70	–																
2	8.06	–																
3	8.06	–																
4	21.84	–																
5	14.45	–																
6	40.32	–																
7	6.05	6.05																
8	8.16	19.0																
9	16.53	24.8																
10	–	9.07																
11	–	4.70																

2.1.2 Расчет накопления готовности проекта

В данном пункте производится оценка текущих состояний работы над проектом.

Введем обозначения:

– ТРобщ. – общая трудоемкость проекта;

– ТРi (ТРk) − трудоемкость i-го (k-го) этапа проекта, $\boldsymbol{i = \overline{1, I}}$;

– ТРiН − накопленная трудоемкость i-го этапа проекта по его завершении;

– ТРij (ТРkj) − трудоемкость работ, выполняемых j-м участником на i-м этапе, здесь $\boldsymbol{j = \overline{1, m}}$ − индекс исполнителя.

Степень готовности определяется формулой:

$$СГ_i = \frac{ТР_i^{Н}}{ТР_{общ.}} = \frac{\sum_{k=1}^{i} ТР_k}{ТР_{общ.}} = \frac{\sum_{k=1}^{i}\sum_{j=1}^{m} ТР_{km}}{\sum_{k=1}^{I}\sum_{j=1}^{m} ТР_{km}} \quad (2.5)$$

В таблице 6 приведены показатели нарастания технической готовности работы и удельный вес каждого этапа.

Таблица 6 – Нарастание технической готовности работы и удельный вес каждого этапа

Этап	$ТР_i$, %	$СГ_i$, %
Получение исходных данных (логическая, физическая, информационная топология сети, файлы конфигураций)	1.94	1.94
Составление и утверждение ТЗ	4.23	6.16
Изучение функциональных характеристик существующего оборудования, линий связи, используемых протоколов	4.23	10.39
Изучение конфигурационных файлов устройств. Поиск ошибок конфигурации топологии, оборудования	11.44	21.83
Изучение текущего состояния рынка сетевого оборудования, протоколов. Изучение возможности замены устаревшего оборудования на новое.	7.57	29.40

Продолжение таблицы 8

Составление модели сети с учетом внесенных исправлений в её архитектуру.	21.13	50.53
Тестирование модели сети. Устранение ошибок.	6.34	56.87
Разработка плана внедрения проекта у заказчика. Составление сопроводительной документации.	14.26	71.13
Монтажные работы (установка оборудования, прокладка линий связи)	21.65	92.78
Тестирование новой конфигурации	4.75	97.54
Сдача проекта заказчику	2.46	100.00

2.2 Расчет сметы затрат на выполнение проекта

В данном разделе приведен расчет сметной стоимости выполнения разработки по следующим статьям затрат:

- материалы и покупные изделия;
- заработная плата;
- социальный налог;
- расходы на электроэнергию (без освещения);
- амортизационные отчисления;
- прочие услуги (сторонних организаций);
- прочие (накладные расходы) расходы.

2.2.1 Расчет материальных затрат

Расчет материальных затрат (в т. ч. оборудование, расходные материалы, работы по монтажу оборудования) требует отдельного согласования и не включается в данном разделе.

2.2.2 Расчет заработной платы

Среднедневная тарифная заработная плата ($ЗП_{дн-т}$) рассчитывается по формуле:

$$ЗП_{дн\text{-}т} = МО/20.58 \quad (2.6)$$

учитывающей, что в году 247 рабочих дней и, следовательно, в месяце в среднем 20.58 рабочих дня (при пятидневной рабочей неделе).

Для перехода от тарифной (базовой) суммы заработка исполнителя, связанной с участием в проекте, к соответствующему полному заработку (зарплатной части сметы) необходимо первую умножить на интегральный коэффициент $К_и$ = 1,1* 1,133*1,3 = 1,62. Таблица 7 показывает смету расчет сметы затрат за заработную плату.

Таблица 7 – Затраты на заработную плату

Исполнитель	Оклад, руб./мес.	Среднедневная ставка, руб./раб.день	Затраты времени, раб.дни	Коэффициент	Фонд з/платы, руб.
ИР	7864.11	382.12	91	1.62	**56332.13**
ИВ	7864.11	382.12	46	1.62	**28475.58**
Итого:					**84807.71**

2.2.3 Расчет затрат на социальный налог

Затраты на единый социальный налог (ЕСН), включающий в себя отчисления в пенсионный фонд, на социальное и медицинское страхование, составляют 30 % от полной заработной платы по проекту, т.е. $С_{соц.} = С_{зп}$*0,3. Итак, в нашем случае $С_{соц.}$ = 84807.71* 0,3 = 25442.31 руб.

2.2.4 Расчет затрат на электроэнергию

Данный вид расходов включает в себя затраты на электроэнергию, потраченную в ходе выполнения проекта на работу используемого оборудования, рассчитываемые по формуле:

$$С_{эл.об.} = Р_{об} \cdot t_{об} \cdot Ц_Э \quad (2.7)$$

где $Р_{ОБ}$ – мощность, потребляемая оборудованием, кВт;

$Ц_Э$ – тариф на 1 кВт·час;

$t_{об}$ – время работы оборудования, час.

Для ТПУ $Ц_Э$ = 5.257 руб./квт·час (с НДС).

Время работы оборудования вычисляется на основе итоговых данных таблицы (Таблица 4) для инженера (ТРД) из расчета, что продолжительность рабочего дня равна 8 часов.

$$tоб = ТРД * Kt \quad (2.8)$$

где Kt ≤ 1– коэффициент использования оборудования по времени, равный отношению времени его работы в процессе выполнения проекта к ТРД, и определен значением 0.6.

Мощность, потребляемая оборудованием, определяется по формуле:

$$Р_{ОБ} = Р_{ном.} * К_С \quad (2.9)$$

где $Р_{ном.}$ – номинальная мощность оборудования, кВт;

$К_С \leq 1$ – коэффициент загрузки, зависящий от средней степени использования номинальной мощности. Для технологического оборудования малой мощности $К_С = 1$.

Таблица 8. Затраты на электроэнергию технологическую

Наименование оборудования	Время работы оборудования $t_{ОБ}$, час	Потребляемая мощность $P_{ОБ}$, кВт	Затраты $Э_{ОБ}$, руб.
Ноутбук	1138*0.6	0.057	204.6
Струйный принтер	3	0.1	1.58
Итого:			**206.18**

2.2.5 Расчет прочих расходов

В статье «Прочие расходы» отражены расходы на выполнение проекта, которые не учтены в предыдущих статьях, их следует принять равными 10% от суммы всех предыдущих расходов, т.е. Спроч. = (Сзп + Ссоц + Сэл.об. + Сам + Снп) * 0,1 = (84807.71+25442.31+206.18) * 0.1 = 11045.62

2.2.6 Расчет общей себестоимости разработки

Проведя расчет по всем статьям затрат на разработку, можно определить общую себестоимость проекта. Итоговый результат отображен в таблицеТаблица **9**).

Таблица 9. Затраты на разработку проекта

Таким образом, затраты на разработку составили С = **121501.82** руб.

2.2.7 Расчет прибыли

Так как мы не располагаем данными для применения «сложных» методов, то прибыль примем в размере 20% от полной себестоимости проекта. Таким образом, прибыль составит: 121501.82 * 0.2 = 24300.36 руб.

2.2.8 Расчет НДС

НДС составляет 18% от суммы затрат на разработку и прибыли. В нашем случае это (121501.82 + 24300.36) * 0.18 = 26244.39 руб.

2.2.9 Цена разработки НИР

Цена равна сумме полной себестоимости, прибыли и НДС, в нашем случае $Ц_{НИР(КР)}$ = 121501.82 + 24300.36 + 26244.39 = 172046.57 руб.

2.3 Оценка экономической эффективности проекта

Оценка экономической эффективности проекта связана с оценкой снижения риска осуществления угроз информационной безопасности благодаря модернизации технической инфраструктуры. Такая оценка требует применения сложных комплексных методик и привлечения высококвалифицированных специалистов. Подобные расчеты требует отдельного трудоемкого исследова-

ния и выходят за рамки данной работы. Стоит, однако, сказать, что с внедрением проектируемой системы значительно снижаются риски, связанные с информационной безопасностью, а значит можно говорить о положительном экономическом эффекте проекта.

2.3.1 Оценка научно-технического уровня НИР

Научно-технический уровень характеризует влияние проекта на уровень и динамику обеспечения научно-технического прогресса в данной области. Для оценки научной ценности, технической значимости и эффективности, планируемых и выполняемых НИР, используется метод балльных оценок. Балльная оценка заключается в том, что каждому фактору по принятой шкале присваивается определенное количество баллов. Обобщенную оценку проводят по сумме баллов по всем показателям. На ее основе делается вывод о целесообразности НИР.

На основе оценок признаков работы определим интегральный показатель ее научно-технического уровня по формуле:

$$K_{\text{НТУ}} = \sum_{i=1}^{3} R_i \cdot n_i \qquad (2.14)$$

где $I_{\text{НТУ}}$ – интегральный индекс научно-технического уровня;

R_i – весовой коэффициент i-го признака научно-технического эффекта;

n_i – количественная оценка i-го признака научно-технического эффекта, в баллах.

Таблица 10 – Оценки научно-технического уровня НИР

Значимость	Фактор НТУ	Уровень фактора	Выбранный балл	Обоснование выбранного балла
0,4	Уровень новизны	Относительно новая	4	Основную часть балла составляет разработка метода и устройства обнаружения вторжения в линию связи

0,1	Теоретический уровень	Разработка способа	6	Описанный способ был ранее представлен, но его применение не было распространено на линии связи ЛВС
0,5	Возможность реализации	В течение первых лет	10	Внедрение основной части проекта (обновление оборудования) занимает около месяца. Разработка и внедрение устройства потребует времени до 1-2 лет

Список публикаций студента

1. Бахтин А.О., Шерстнёв В.С., Шерстнёва А.И.; АНАЛИЗ УЯЗВИМОСТИ В ИНТЕРПРЕТАТОРЕ bash – Shellshock // Современные наукоемкие технологии. – 2015. – № 4. – С. 7-11; URL: http://www.top-technologies.ru/ru/article/view?id=35005 (дата обращения: 07.04.2016)

2. Бахтин А.О., Шерстнёв В.С., Пичугова И.Л.; Detection of an Unauthorized Wired Connection to a Local Area Network by Solving Telegraph Equations System // XII Международная IEEE Сибирская конференция по управлению и связи (SIBCON-2016); URL: http://ieee.tpu.ru/hse/papers/623fu1c.pdf (дата обращения: 22.05.2016)